## **ABSTRACT**

"A Method of Exchanging Digital Data"

A method of exchanging digital signatures (sign\_A, sign\_B) between a first and a second party (A,B) includes the first party (A) encrypting their signature (sign A) and generating an certificate (Cert A), authentication authentication the certificate (Cert A) authenticating that the encrypted signature (C\_T) is an encryption of the signature (sign\_A). The first party (A) sends the encrypted signature (C T) and the authentication certificate (Cert A) to the second party (B). The second party (B) verifies that the encrypted signature (C T) is an encryption of the digital signature (sign A) of the first party (A), and if the verification is positive, the second party (B) sends its digital signature (sign B) to the first party (A). The first party (A) verifies that the digital signature (sign B) is the digital signature of the second party (B), and if the verification is positive the first party sends its unencrypted signature (sign\_A) to the second party (B). The second party (B) verifies that the digital signature (sign\_A) is the first party's digital signature, and accepts the digital signature (sign A) if the verification is positive. If the verification is negative, the second party (B) sends the encryted digital signature (C T) and its digital signature (sign B) to a third party (T). The third party (T) independent of the first and second parties (A,B) and has a decryption key to decrypt the encrypted digital signature (C\_T) of the first party (A).

3.1

The third party (T) decrypts the encrypted digital signature (C\_T) to obtain the first party's digital signature (sign\_A), and verifies that the digital signatures (sign\_A, sign\_B) are the digital signatures of the first and second party (A,B) respectively. If both digital signatures (sign\_A, sign\_B) are verified as the digital signatures of the first and second parties (A,B), the third party (T) sends the first party's digital signature (sign\_A) to the second party (B) and sends the second party's digital signature (sign\_B) to the first party (A).

## Figure 1